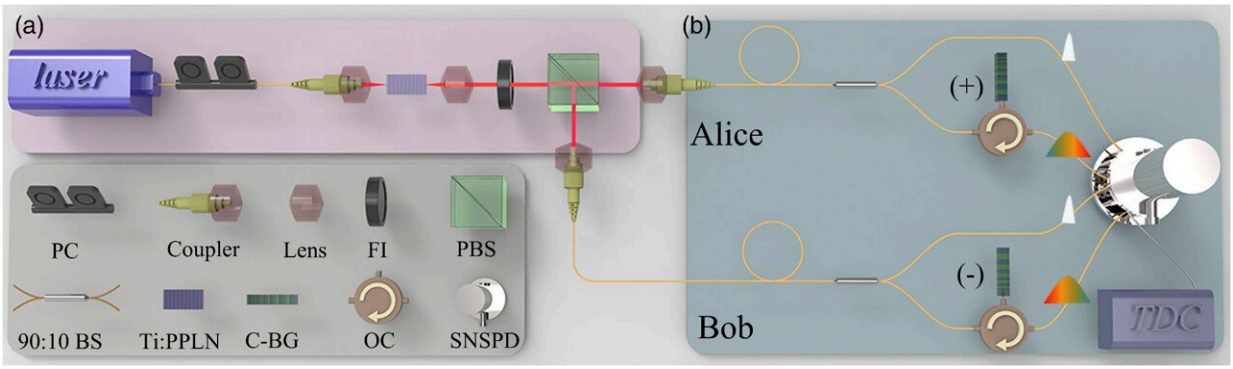
Quantum random number generator operates securely and independently of source devices

May 17 2023



Experimental setup of the source-DI QRNG. (a) Entanglement source: the time–energy entangled photon pairs are generated from the Ti:PPLN waveguide pumped by a pulsed laser with a duration of 5 ns, which are separated by a PBS. (b) Measurement device: photons are passively selected for measurement Tδ or Dδ by a 90:10 beam splitter (BS) after being coupled to fiber in Alice and Bob sides. PC, polarization controller; FI, filter; C-BG, chirped Bragg grating; OC, optical circulator; SNSPD, superconducting nanowire single-photon detector; and TDC, time-to-digital converter. Credit: *Advanced Photonics* (2023). DOI: 10.1117/1.AP.5.3.036003

Quantum random number generators (QRNGs) produce genuine randomness based on the inherent unpredictability of quantum mechanics. They have important applications in quantum information processing and computation tasks. In practice, any imperfection or inaccurate characterization of quantum source devices in a real

implementation highly affects the security and generation rate of QRNGs, and may even induce the disappearance of quantum randomness.

Source-device-independent (source-DI) QRNGs operate with untrusted sources yet well characterized measurement devices, to positively address these problems.

As reported in *Advanced Photonics*, researchers from Nanjing University recently proposed and experimentally demonstrated a secure and fast source-DI QRNG protocol that is simple and efficient for practical implementation. The source-DI QRNG in this work is realized through single-photon detection technology assisted by entangled photons.

The random numbers are extracted by a process that measures the arrival time of a photon from a pair of time–energy entangled photons. The time–energy entangled photon pairs are produced from a spontaneous parametric down conversion (SPDC) process.

The researchers were able to confirm the security of the scheme by certifying the time–energy entanglement though observation of nonlocal dispersion cancelation. To improve security, they employ a modified entropic uncertainty relation to quantify the randomness, taking into account a well-recognized problem of finite measurement range.

They report a secure generation rate of random bits at 4 megabits per second (Mbps), which they note could reach the level of giga bps with advanced single-photon detectors, given their faster detection speed and lower temporal resolution. Based on a PPLN waveguide SPDC source, the source-DI QRNG they realized may be further developed as an integrated chip-scale device by exploring on-chip photon generation, manipulation, and detection techniques.

According to the corresponding author Yan-Xiao Gong, Professor at Nanjing University, "Compared with several existing semi-DI QRNGs, our work achieves an excellent balance among security, speed, and practicality." He adds, "This research paves the way for practical applications of secure quantum information tasks and promotes the development of high-performance and high-security quantum random number generators."

More information: Ji-Ning Zhang et al, Realization of a source-device-independent quantum random number generator secured by nonlocal dispersion cancellation, *Advanced Photonics* (2023). DOI: 10.1117/1.AP.5.3.036003

Provided by SPIE